Algebra 1

Prof. A. D'Andrea, A. De Sole, G. Mondello

Prova scritta del 17-2-2022

Nome e Cognome: _____

Numero di Matricola: _____

Docente: **D'Andrea \ De Sole - Mondello** (cerchiare il/i docente/i).

Esercizio	Punti totali	Punteggio
1	6	
2	6	
3	6	
4	6	
5	6	
Totale	30	

Esercizio 1. Sia G il gruppo delle matrici 3×3 triangolari superiori e invertibili a coefficienti nel campo $\mathbb{F}_2$ con due elementi.

(a) Calcolare l'ordine di G.

(b) Spiegare perché G abbia centro non banale.

(c) Esibire almeno un elemento di ordine 4 in G.

Soluzione: Il determinante di una matrice triangolare superiore è il prodotto degli elementi sulla diagonale principale. Affinché una matrice triangolare superiore sia invertibile è pertanto necessario che gli elementi sulla diagonale principale siano diversi da 0. Nel campo $\mathbb{F}_2$ questo vuol dire che sono tutti uguali ad 1. La verifica che le matrici 3×3 triangolari superiori a coefficienti in $\mathbb{F}_2$ con 1 sulla diagonale è immediata, e inoltre segue dal testo dell'esercizio: possiamo quindi saltarla con serenità.

(a) Dobbiamo contare le matrici descritte sopra. Possiamo scegliere liberamente, per ciascun coefficiente al di sopra della diagonale principale, uno dei due valori di $\mathbb{F}_2$. Le possibili scelte sono allora $2 \cdot 2 \cdot 2 = 8$ e il gruppo G ha ordine 8.

(b) Il gruppo G è non abeliano, come si verifica direttamente calcolando, ad esempio:

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Abbiamo visto a lezione che un gruppo non abeliano di ordine p^3, con p primo, ha centro di ordine p, e questo fatto è quindi valido anche per il gruppo G, che ha centro di ordine 2.

Non è difficile, e lo avete fatto in molti, calcolare l'elemento centrale di G diverso dall'identità, che è

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

IMPORTANTE: alcuni di voi hanno sostenuto che un elemento di ordine 2 in G è necessariamente centrale. Questo è falso. Ad esempio, l'elemento

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

ha ordine 2, ma non è centrale.

(c) Gli elementi di ordine 4 in G sono due, e più precisamente

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

IMPORTANTE: per mostrare che hanno ordine 2 non basta calcolarne la quarta potenza e verificare che coincide con l'identità. Questo fatto vi garantisce solo che l'ordine DIVIDE 4. Dovete poi far vedere che non è 2 (che non sia 1 è ovvio: perché?) calcolandone il quadrato.

Per la cronaca, il gruppo G è isomorfo al diedrale del quadrato (i gruppi non abeliani di ordine 8 sono isomorfi a tale gruppo OPPURE al gruppo delle unità dei quaternioni, ma quest'ultimo ha sei elementi di ordine 4).

Esercizio 2. Sia G un gruppo di ordine finito e sia $H \subset G$ un sottogruppo di indice $[G : H] = p$ primo. Dimostrare che H è normale oppure ci sono esattamente p sottogruppi di G coniugati a H.

Soluzione: il numero dei coniugati di un sottogruppo H di un gruppo G coincide con l'indice del suo normalizzatore $N(H)$, che contiene H. Poiché

$$[G : H] = [G : N(H)] \cdot [N(H) : H],$$

si vede subito che $[G : N(H)]$ è un divisore di $[G : H] = p$. Se è 1, allora $N(H) = G$ e H è normale. Se è p, allora H ha p coniugati.

IMPORTANTE: in questa situazione, H non è mai un p-Sylow di G, poiché l'indice di un p-Sylow di G è un numero che non ha p nella sua fattorizzazione in primi. Chiunque abbia detto questa cosa ha detto il falso. Inoltre non potete supporre che $|H|$ sia un numero primo, poiché è facile trovare controesempi a questa affermazione.

Esercizio 3. Si consideri l'omomorfismo di anelli $\phi : \mathbb{Z}[x] \to \mathbb{R}$ definito da $x \mapsto \frac{1}{2} + \sqrt{2}$. Mostrare che il nucleo è un ideale principale e determinarne un generatore.

Soluzione: innanzitutto $\mathbb{Z}[x]$ non è un dominio euclideo, né un dominio a ideali principali. Sono anelli di questo tipo i $K[x]$ con K campo, ma $\mathbb{Z}$ non è un campo!!!

Cerchiamo un polinomio che annulli $\alpha = \frac{1}{2} + \sqrt{2}$. Si ha $2\alpha - 1 = 2\sqrt{2}$, da cui $(2\alpha - 1)^2 - 8 = 0$. Semplificando, si vede che $4x^2 - 4x - 7$ annulla α. Potete chiaramente scrivere anche $x^2 - x - 7/4$, ma ricordate che state lavorando in $\mathbb{Z}[x]$, quindi è bene che i polinomi abbiano coefficienti interi! Il polinomio $4x^2 - 4x - 7 \in \mathbb{Z}[x]$ è primitivo, ed è anche irriducibile in $\mathbb{Z}[x]$, poiché non ha radici razionali (che sarebbero inevitabili se riusciste a fattorizzarlo nel prodotto di due polinomi di primo grado). Il nostro obiettivo ora è quello di mostrare che $\ker \phi = (4x^2 - 4x - 7)$.

Se $f(x) \in \ker \phi$, allora $f(x)$ è un polinomio a coefficienti interi (e quindi razionali) che annulla α. E' importante notare che $4x^2 - 4x - 7$ è il polinomio minimo di α su $\mathbb{Q}$, in quanto è irriducibile in $\mathbb{Q}[x]$ (per il motivo di prima). Allora $f(x) \in \mathbb{Z}[x]$ è multiplo di $4x^2 - 4x - 7$ in $\mathbb{Q}[x]$. Una delle forme del Lemma di Gauss viste a lezione ci garantisce allora che $4x^2 - 4x - 7$ divide $f(x)$ anche in $\mathbb{Z}[x]$, o equivalentemente $f(x) \in (4x^2 - 4x - 7)$.

Questo mostra che $\ker \phi \subset (4x^2 - 4x - 7)$, mentre l'altra inclusione segue da $4x^2 - 4x - 7 \in \ker \phi$.

IMPORTANTE: non è vero che un polinomio (diciamo primitivo di grado 2 o 3) a coefficienti in $\mathbb{Z}$ sia irriducibile non appena abbiamo verificato che non abbia radici in $\mathbb{Z}$. Ad esempio, $4x^2 - 1$ non ha radici intere, ma si fattorizza come $4x^2 - 1 = (2x - 1)(2x + 1)$. Per poter utilizzare il ragionamento dovete verificare che non ha radici RAZIONALI e poi usare il fatto che una fattorizzazione non banale produrrebbe una radice razionale. Inoltre tutte le proprietà che abbiamo visto a lezione sul polinomio minimo di un algebrico riguardano il polinomio minimo a coefficienti nel campo base. Se il campo base non è un campo, come in questo caso, dovete stare un po' attenti.

Un'ultima cosa: non potete fare la divisione euclidea in $\mathbb{Z}[x]$, altrimenti riuscireste a mostrare che $\mathbb{Z}[x]$ è un dominio euclideo, mentre non lo è. In generale, se $a(x), b(x) \in \mathbb{Z}[x]$ E $b(x)$ E' UN POLINOMIO MONICO, potete trovare $q(x), r(x) \in \mathbb{Z}[x]$ tali che $a(x) = b(x)q(x) + r(x)$ con $r(x)$ nullo o di grado inferiore a quello di $b(x)$, ma nel nostro caso $4x^2 - 4x - 7$ non è monico, e non potete dare per scontato che il resto abbia grado inferiore. L'unica strada percorribile è attraverso il Lemma di Gauss.

Esercizio 4. Sia $L \subset \mathbb{Z}^2$ il reticolo generato dai vettori $v_1 = (3,4)^T$ e $v_2 = (2,5)^T$. Determinare l'indice di L in $\mathbb{Z}^2$. Determinare delle basi $\mathcal{B} = (e_1, e_2)$ di $\mathbb{Z}^2$ e interi positivi d_1, d_2 tali che $(d_1 e_1, d_2 e_2)$ sia una base di L.

Soluzione: l'indice di un sottogruppo L in un gruppo abeliano G è l'ordine del quoziente G/L, quindi se sapete dire come è fatto $\mathbb{Z}^2/L$ avete concluso. Si procede come al solito con la diagonalizzazione à la Smith, che fornisce

$$\begin{pmatrix} 3 & 2 \\ 4 & 5 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 3 & 2 \\ 1 & 3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 3 \\ 3 & 2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 3 \\ 0 & -7 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 0 & -7 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 0 & 7 \end{pmatrix}.$$

Gli interi d_1, d_2 sono quindi $d_1 = 1, d_2 = 7$ e l'indice di L in $\mathbb{Z}^2$ è il loro prodotto $1 \cdot 7 = 7$. Notate come, nelle manipolazioni di diagonalizzazione, il determinante cambi al più del segno, e quindi l'indice si poteva ricavare fin dall'inizio calcolando il (valore assoluto del) determinante della matrice iniziale, che era proprio 7.

Il calcolo dei vettori e_1, e_2 è lievemente più complicato, e può essere fatto come abbiamo visto a lezione. Tuttavia, in questo caso, ci troviamo in $\mathbb{Z}^2$ e possiamo anche fare i conti con le mani! Possiamo completare il vettore $e_1 = v_1 = (3,4)^T$ ad una base di $\mathbb{Z}^2$ scegliendo un secondo vettore che dia una matrice 2×2 di determinante ± 1, come ad esempio $e_2 = (1,1)$. Con semplici conti, ora si vede che $v_2 = (2,5)^T = 3e_1 - 7e_2$ e quindi il sottogruppo L, che è generato da v_1 e v_2, è anche generato da e_1 e $7e_2$.

IMPORTANTE: se nelle vostre manipolazioni sommate o sottraete ad una riga/colonna un multiplo RAZIONALE e non intero di un'altra riga/colonna, state sbagliando.

PS: Volendo proprio procedere come visto a lezione, mettiamo la matrice iniziale in forma di Smith privilegiando le manipolazioni per colonna. Allora da

$$\begin{pmatrix} 3 & 2 \\ 4 & 5 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 \\ -1 & 5 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ -1 & 7 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 0 & 7 \end{pmatrix},$$

dove abbiamo prima sottratto alla prima colonna la seconda, poi alla seconda colonna due volte la prima e poi, finalmente, sommato alla seconda riga la prima riga, otteniamo

$$L = \begin{pmatrix} 3 & 2 \\ 4 & 5 \end{pmatrix} \mathbb{Z}^2 = \begin{pmatrix} 1 & 2 \\ -1 & 5 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \mathbb{Z}^2 = \begin{pmatrix} 1 & 2 \\ -1 & 5 \end{pmatrix} \mathbb{Z}^2 = \begin{pmatrix} 1 & 0 \\ -1 & 7 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \mathbb{Z}^2 = \begin{pmatrix} 1 & 0 \\ -1 & 7 \end{pmatrix} \mathbb{Z}^2$$

e quindi

$$L = \begin{pmatrix} 1 & 0 \\ -1 & 7 \end{pmatrix} \mathbb{Z}^2 = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 7 \end{pmatrix} \mathbb{Z}^2,$$

il che vuol dire – leggendo per colonne! – che nella base $e_1 = (1,-1)^T, e_2 = (0,1)^T$ il sottogruppo L è generato da $e_1, 7e_2$.

Esercizio 5. Si consideri il polinomio $f(x) = x^3 + x + 1 \in \mathbb{Q}[x]$ e siano $\alpha, \beta, \bar{\beta}$ le sue tre radici, con $\alpha \in \mathbb{R}$ e $\bar{\beta} \neq \beta \in \mathbb{C}$. Sia $\mathbb{K} \subset \mathbb{C}$ il campo di spezzamento di $f(x)$ su $\mathbb{Q}$.

(a) Determinare il grado di $\mathbb{K}$ su $\mathbb{Q}$.

(b) Dire se $\sqrt{29}$ appartenga a $\mathbb{K}$.

(c) Mostrare che α^2 ha grado 3 su $\mathbb{Q}$ e determinare il polinomio irriducibile $g(x)$ per α^2 su $\mathbb{Q}$.

Soluzione: innanzitutto, il polinomio primitivo $f(x)$ è irriducibile in $\mathbb{Q}[x]$, e quindi anche in $\mathbb{Z}[x]$ per il Lemma di Gauss, poiché ha grado 3 e non ha radici razionali. Le uniche potrebbero essere ± 1, ma si vede subito che non soddisfano $f(x)$. Segue immediatamente che $f(x)$ è il polinomio minimo sia di α che di $\beta, \bar{\beta}$ su $\mathbb{Q}$.

(a) Il campo di spezzamento $\mathbb{K}$ contiene sicuramente $\mathbb{Q}(\alpha)$ che ha grado 3 su $\mathbb{Q}$ in quanto $f(x)$ è il polinomio minimo di α su $\mathbb{Q}$. Tuttavia $\beta \notin \mathbb{Q}(\alpha)$ poiché $\beta \notin \mathbb{R}$, mentre $\mathbb{Q}(\alpha) \subset \mathbb{R}$.

Pertanto $[\mathbb{K} : \mathbb{Q}] = [\mathbb{K} : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] > 1 \cdot 3 = 3$ ed è un multiplo di 3. Abbiamo visto a lezione che il grado del campo di spezzamento di un polinomio irriducibile di grado n è $\leq n!$ e questo ci fa concludere che $[\mathbb{K} : \mathbb{Q}] = 6$.

(b) Se $\sqrt{29} \in \mathbb{K}$, allora $\mathbb{Q}(\alpha, \sqrt{29}) \subset \mathbb{K}$ contiene i sottocampi $\mathbb{Q}(\alpha)$ e $\mathbb{Q}(\sqrt{29})$, che hanno grado $3, 2$ su $\mathbb{Q}$. Pertanto $[\mathbb{Q}(\alpha, \sqrt{29}) : \mathbb{Q}]$ è multiplo di 6 e divide $[\mathbb{K} : \mathbb{Q}] = 6$ e quindi $\mathbb{Q}(\alpha, \sqrt{29}) = \mathbb{K}$.

Ma allora ogni elemento di $\mathbb{K}$ sarebbe reale, mentre abbiamo visto prima che così non è.

(c) Si può fare in molti modi, ma il più immediato è il seguente: poiché $\alpha^3 + \alpha = -1$, quadrando si ottiene

$$(\alpha^2)^3 + 2(\alpha^2)^2 + \alpha^2 = \alpha^6 + 2\alpha^4 + \alpha^2 = 1.$$

Ma allora α^2 soddisfa il polinomio $g(x) = x^3 + 2x^2 + x - 1$ che si vede facilmente essere irriducibile in $\mathbb{Q}[x]$, con le solite tecniche, in quanto privo di radici razionali.

IMPORTANTE: I sottocampi $\mathbb{Q}(\alpha), \mathbb{Q}(\beta), \mathbb{Q}(\bar{\beta}) \subset \mathbb{K} \subset \mathbb{C}$ sono diversi l'uno dall'altro, anche se $\alpha, \beta, \bar{\beta}$ hanno tutti lo stesso polinomio minimo. In effetti, si vede facilmente che $\beta, \bar{\beta} \notin \mathbb{Q}(\alpha)$ poiché gli elementi di $\mathbb{Q}(\alpha)$ sono tutti reali. Mostrare che $\mathbb{Q}(\beta) \neq \mathbb{Q}(\bar{\beta})$ è lievemente più complicato, ma si può procedere così: se $\bar{\beta} \in \mathbb{Q}(\beta)$, allora $\beta + \bar{\beta} \in \mathbb{Q}(\beta)$. Non è complicato convincersi che $\beta + \bar{\beta} = -\alpha$, ma allora $\mathbb{Q}(\beta)$ conterrebbe tutte e tre le radici di $x^3 + x + 1$, e ne sarebbe il campo di spezzamento, mentre abbiamo visto che il campo di spezzamento $\mathbb{K}$ ha grado 6 su $\mathbb{Q}$.

IMPORTANTE: per mostrare che $\sqrt{29} \notin \mathbb{K}$ non è sufficiente far vedere che $\sqrt{29}$ non soddisfa $f(x)$. In effetti, $\mathbb{K}$ contiene infiniti elementi, ma le radici di $f(x)$ sono soltanto tre. Per la cronaca, $\mathbb{K}$ contiene $\sqrt{-31}$, quindi molti degli argomenti che avete proposto per risolvere il secondo punto DEVONO fallire.